BALTIMORE COUNTY, MARYLAND
REQUEST FOR PROPOSAL NO. P-10000046
SOFTWARE, ELECTRONIC HEALTH RECORDS AND MANAGEMENT SYSTEM

ATTACHMENT H
OIT WORKSHEET QUESTIONNAIRE

This worksheet is provided in Word format to allow Contractor to insert answers below each question. Contractor to provide the completed worksheet with their Technical Proposal.

G1 Describe what methods your company uses to keep up with changes in your target industry.

G2 Identify any scalability constraints within the proposed solution.

G3 What is the largest organization you support? Please describe this organization and the setup/use of your system in this environment.

G4 Explain any plans for major technology or functionality changes in the proposed product within the next 18 to 24 months.

G5 Describe your company's testing and quality assurance process.

G6 Has the proposed solution release undergone formal testing utilizing a formal test plan? Are these test plans available for review?

G7 Describe any administrative remote access features in the proposed solution.

G8 Describe any electronic notification features within the proposed solution, integration with an enterprise monitoring system (such as encountered problems, issues, and performance.)

G9 Define the open architecture model on which the proposed solution was developed.

G10 Describe the abilities within the proposed solution to archive, retrieve, and purge information.

G11 Describe error logging and reporting within the proposed solution.

G12 Describe the license structure available for the proposed solution (including named user, concurrent user, entreprise, and any other licences.)

G13 Identify any third party products proposed in your solution. Is Contractor planning to use third party contractors to meet any requirements from this proposal? Contractor needs to identify, in detail, any third party contractors and/or relationships.

Security

S1 How do you determine which employees have access to County data?

S2 Does Contractor have a policy in place which mandates employees notify them of any criminal charges or offenses?

S3 Does the application utilize FIPS 140-2 validated encryption algorithms for all communications in transit? If so, provide the corresponding validation certificate. (Transmission Confidentiality and Integrity, Cryptographic Protection)

S4 Does the application utilize FIPS 140-2 validated encryption algorithms to store data at rest? If so, provide the corresponding validation certificate. (Transmission Confidentiality and Integrity, Cryptographic Protection)

S5 Does the application have the capability to display a Standard Mandatory Consent Banner before granting access to the application? (Access Control – System Use Notification)

S6 The OWASP Top 10 identifies the top 10 most critical web application security flaws (https://www.owasp.org/index.php/Top_10_2013-Top_10). How does your organization address and mitigate the common risks identified in the top 10. (Risk Assessment)

S7 Describe the Information Security Architecture philosophy, requirements, and approach taken to ensure confidentiality, integrity and availability of customer data? (Information Security Architecture)

Access Control

AC1 What method(s) of access control does the application provide (Role Based, Mandatory, or Discretionary)?

AC2 Can access control be controlled by Active Directory / LDAP / ADFS / SAML?

AC3 Does the solution provide the capability and functionality to authenticate users with multifactor authentication? (Identification and Authentication (Organizational Users))

AC4 How granular can the access control mechanism be to restrict functionality (including but not limited to role, user, screen, module, table, column, update, view only, field.)?

AC5 Does the application provide a capability to limit the number of logon sessions per user? (Access Control – Inactivity Logoff)

AC6 Does the application automatically terminate privileged and non-privileged sessions after 15 min of idle time? (Access Control – Inactivity Logout, Session Lock)

AC7 Can the application be run in a user context without the need for privileged access on the local system? (Access Control – Least Privilege)

AC8 Can the application adequately detect and stop or limit data mining attempts? (Access Control – Data Mining Protection)

AC9 What capability and functionality does the offering provide and restrict access to mobile devices? (Access Control for Mobile Devices)

AC10 If the solution cannot integrate with the Baltimore County IDP can the system enforce County standards for identification and authentication (password complexity, length, cryptographically protected, reuse limits, etc). (Authenticator Management)

AC11 Are application vulnerability assessments performed routinely by a qualified third party and are the results of those test available for review? (Risk Assessment)

Audit and Accountability

AA1 Does the application have the capability to time correlated audit events for the following actions (Content of Audit Records):

- Account Creation
- Account Modification
- Account Disabling Actions
- Account Enabling Actions
- Account Deletion Actions
- Group Membership Changes

- Successful Logins
- Failed Logins
- Start and End Times of System Access
- Privileged Account Usage
- Privileged Account Changes
- Configuration Changes
- Application Events

AA2 If this is a web based application does the application provide audit record generation capability for HTTP headers including User-Agent, Referrer, GET and POST with destination IP address? (Content of Audit Records)

AA3 How does the application prevent altering of audit data? (Protection of Audit Information)

AA4 How long are audit events retained? (Audit and Accountability – Audit Storage Capability, Audit Record Retention)

AA5 Does the application provide log data reduction and reporting capabilities within the application? (Audit Reduction and Report Generation)

AA6 How does the application have the capability to react to failed login attempts and is this action configurable? (Audit Events)

AA7 **If a hosted solution** Does the application vendor (or sub contracted vendor) have a SOC 2 type 2 report available for review and will the vendor provide updated copies of the report after every yearly review? (Security Assessments, Continuous Monitoring)

Awareness and Training

AT1 Are vendor employees provided security awareness training and if so how long are the logs of training maintained? (Awareness and Training – Security Awareness)

Configuration Management

CM1 Is there a Configuration Management process in place to ensure that changes to the Platform or Software are communicated prior to implementation?
(Configuration Management Policies and Procedures)

Contingency Planning

CP1 Does the vendor have established and tested contingency plans in place to meet stated Service Level Agreement timelines for availability? (Contingency Plan Testing)

- Business Continuity Plans
- Disaster Recovery Plans
- Continuity of Operations Plans
- Crisis Communications Plans
- Cyber Incident Response Plans
- (Contingency Plan Testing)

CP2 What is your backup and restoration policy and procedure?

Incident Response

IR1 Describe your incident response plan from discovery until closure? (Incident Response Training, Incident Response Testing, Incident Handling)

Maintenance

M1 How often is maintenance performed and is it performed on a routine predictable cycle? (Timely Maintenance)

Media Protection

MP1 What occurs to storage utilized by County data at end of life, is it sanitized in accordance with NIST 800-88? (Media Sanitization)

Personnel Security

PS1 What controls are in place to ensure that employees and sub-contractors are held accountable for the security and standards of use of the system? Including screening of employees. (Personnel Security – Personnel Security Policy and Procedures)

PS2 Are access agreement policies and procedures in place to ensure access to customer data is limited to only when consent is explicitly given? (Personnel Security – Access Agreements)

System and Communications Protection

SC1 How does the system separate user functionality from information system management functionality physically or logically? (Application Partitioning)

SC2 In a multi-tenant environment, how does the system prevent unauthorized and unintended information transfer via shared resources? (Information on Shared Resources, Boundary Protection, Process Isolation)

SC3 How does the system prevent Denial of Service? (Denial of Service Protection, Resource Availability)

System and Information Integrity

SI1 What process exist to remediate flaws in the system once they are discovered? (Flaw Remediation)

SI2 What mechanism is employed to detect and eradicate malicious code? (Malicious Code Protection)

SI3 Does the system perform input validation prior to accepting input to prevent injection type attacks? (Information Input Validation)

Hardware, Network and Database

H1 Contractor to provide the minimum and recommended requirements for any required application server(s) for the proposed solution. Specify Windows OS/NOS, service levels/packs required (Windows 2012 R2 minimum), additional software, additional hardware, 32/64 bit, etc.

H2 Contractor to detail the minimum and recommended requirements for client workstations running Windows 10. Specify service levels/packs required, additional software, additional hardware, etc.

H3 Identify the browsers (including versions and service packs) with which the proposed solution has been tested.

H4 Contractor to provide the minimum and recommended requirements for the database server for the proposed solution. Specify OS/NOS, service levels/packs required, and any additional software and hardware.

H5 Define the environment on which the proposed solution runs (two-tier client server, three or n-tier client server, Web browser based environment, etc.)

H6 Provide information regarding solution high availability.

Network

N1 Does the proposed solution work through proxy servers? Indicate the type of proxy servers that have been tested with the proposed solution.

N2 What ports, protocols, and services are required for the application to function properly?

N3 Does the proposed solution run over a Virtual Private Network (VPN)? Identify the broadband methods utilized (Cable Modem, 4G/LTE.).

N4 Has the proposed solution been tested and implemented using Citrix or Microsoft RDS? Citrix Secure Gateway or Microsoft RDS Gateway?

N5 Will the solution work with a storage area network (SAN) CIFS/NFS? Has the solution been tested in this environment?

N6 If remote access to support system implementation or system support is required, describe the methods employed by your company to provide the connectivity and support.

Database

D1 Identify the DBMS that the proposed solution uses (ie .Oracle 12, MS SQL Server 2014).

D2 Describe the database access that your products provide for reporting. Is this access through APIs or direct access?

Methodologies

M1 Describe in detail your company's methodologies with regard to the following:

- Application development
- Quality assurance – including types of tests, test coverage, test plans, defect management plan, patch management, assurances that patches are correct, whether unit test are included within the code, etc.
- Configuration management – including customization management
- Maintaining different environments (development, test, production, training) and which environments are used.
- Version control
- Solution upgrades
- Customizations

Software Business Solutions

SS1 Contractor to describe customizations versus configuration. Is your system configurable to meet the needs of County or will you need to design customizations? Describe your system's capability of configuration vs. customizations. Can you migrate customizations with newer system versions? How does your system work for version updates with regards to customizations?

SS2 If applicable, Contractor to describe work flow screens that can be tailored for the County? Describe your workflow design process and how County would work with you to develop workflow screens.

SS3 Please list current supported web browsers and mobile device operating systems.

SS4 Contractor to explain standards. Does the system support Enterprise Service Bus for enterprise application integration, Service Oriented Architecture (SOA) standards, ADA standards, and RDBMS? Does the system use XML for data representation and messaging? Describe capabilities for pass through messaging.

SS5 Contractor to provide a detailed discussion on the **supporting services**:

- System management methodology
- System implementation and follow-on technical support
- Data conversion methodology
- Migration planning
- Documentation (administrator, end-user, technical, online)
- Maintenance
- Support agreements (including severity levels and response times)
- New release process
- Future release schedule
- Future direction of application proposed
- Bug fixes (describe level of automation of regression testing tools used in releases, emergency fixes, etc.)
- Beta test program (include details on regression testing process)
- National and or regional user groups available to County staff

SS6 Contractor to describe how it maintains compliance with federal and state laws.

Support

SP1 Contractor to describe the maintenance and support services to be provided under the contract resulting from this RFP.

SP2 Describe Contractor's technical support procedures (include escalation processes, hours and methods for receiving support).

SP3 Contractor to provide the detailed procedure it will follow in the event of a data breach with respect to those whose data was breached, include:

- Requirement to notify
- Notification timeframe
- Provision of pertinent breach details
- Circumstances surrounding the breach
- Corrective actions
- Prevention plans

SP4 Describe your issue resolution processes and how you track support. What tracking systems do you use, and is it accessible by the client/customer?

Service Level Agreement Components

SV1 What level of uptime is guaranteed by the contractor of the service?

SV2 What compensation is provided to customers when an SLA is not meet?

SV3 Are maintenance windows or announced disruptions included in the uptime guarantee or are they separate?

SV4 Has the contractor every suspended services to a customer because of a dispute?

Training

T1 Contractor to describe all training activities that will be provided to County. Include what training comes as part of your services and methodology? What type of training do you offer for configuration and customization of software and APIs? Describe system administration training. Describe who does your training. Include any hardware or software used.

T2 Contractor shall describe any end user training or focus group services provided. Contractor to include information on access to training systems/instances and relevant data and technology as applicable.

Project Management

PM01 County requires project management best practices in the performance of all obligations and responsibilities, particularly those prescribed by the Project Management Institute and documented in the Project Management Book of Knowledge, 3rd edition or later. Offeror to identify any concerns with this requirement.

PM02 Offeror to describe its project management lifecycle (PMLC) and software development lifecycle (SDLC) methodologies. Offeror to identify the development framework to include Waterfall, Agile or Hybrid.